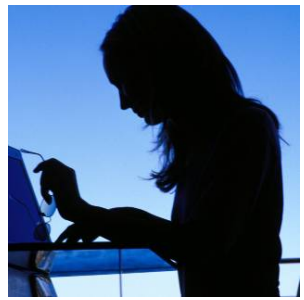



Commercial Funds Transfer Fraud: An Application Provider's Perspective

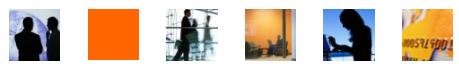
Murray Walton
Chief Risk Officer
Fiserv, Inc.

Democratization of Commercial Funds Transfer

- Formerly, funds transfer offerings were a Big Bank capability, run in-house, aimed at sophisticated commercial customers
- Today, Every Bank wants a competitive solution in the commercial space to retain and attract business clients (and generate fee income), so…
- Application/service providers now offer solutions that allow Every Bank the same cash management capabilities formerly exclusive to Big Bank
- And there is our problem…

Consequences of Democratization

- Expanding commercial funds transfer capabilities from Big Bank to Every Bank increases the number of financial institutions by thousands, the number of end users by millions, and the number of transactions by billions
- Thus, democratization has created a big, ripe target that incents the bad buys to build specialized, exploitive schemes
- Do we believe that Big Bank's systems and processes are more secure and rigorous than Every Bank's? Do we believe Big Bank's customers are more sophisticated and risk-aware?
- We make no such assumptions, but we concede that an expanded ecosystem almost always means greater diversity and greater potential for anomalous outcomes



Commercial Funds Transfer Fraud Primer

The Bad Guys…

- Identify targets, usually accounting or treasury departments of bank customers (or even banks themselves) that routinely execute funds transfers
- Plant key-logging software on targets' computers using social engineering and clever email ("spear phishing")
- Harvest and analyze the capture
- Sell it or use it, often involving third party ("innocent") money mules

Solution: Layered Defenses

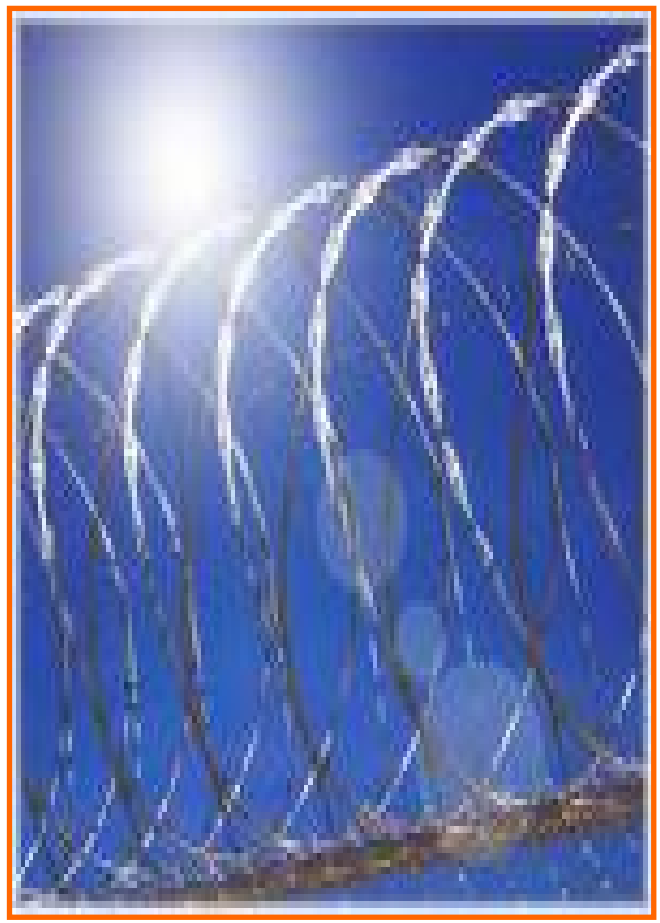
Strengthen Every Link in the Chain…

- Application: Validate soundness through vulnerability scanning and penetration testing
- Hosting: Validate integrity of the environment and the quality of the information security program
- Financial Institutions: Validate strength of control environment including appropriate segregation of duties and solid monitoring and reconciliation processes
- End Users: Validate effectiveness of internal controls and security

Solution: Layered Defenses

Strengthen the Ecosystem…

- Self-updating operating systems, anti-virus and anti-spyware
- Up-to-date application patching
- Securest possible browser settings
- Comprehensive, enforced policies governing use of computing systems, including limits on web browsing, social networking, and third party email
- Robust information security and security awareness programs



Solution: Layered Defenses

Strengthen Authentication…

- Multi-Factor Authentication naiveté
- A cautionary tale about tokens
- In-band vs. out-of-band
- Growing potential for cell phones
- Device fingerprinting
- IP address registration
- Predictive modeling
- Positive Pay

Solution: Layered Defenses

Strengthen Our Resolve…

- Banker Education
- User Education
- Collaboration with Regulatory Agencies and Law Enforcement
- Openness about Challenges
- Call to Action re the Unregulated Side of the Equation: Money Mules and Money Transmitters

The Road Ahead

No Silver Bullet…

- Perpetrators are sophisticated international syndicates operating beyond the reach of any one government
- Cybercrime is now a bona fide profession and industry
- System complexity will continue to grow, and new technologies such as cloud computing will pose challenges and opportunities
- Greed and gullibility will be with us always